Iowa Enterprise Security Policy

Iowa Lunch and Learn Program
April 23, 2002

Kip Peters
Chief Information Security Officer
State of Iowa
515-725-0362
Kip.Peters@itd.state.ia.us
http://www.itd.state.ia.us/security/

Overview

- Security Policy
- Iowa Policy
- Iowa Policy Overview
- Policy Sections
  - Introduction
  - Threats
  - Security Philosophy

Security Policy

- The foundation of an effective information security program
- Source for standards, processes, procedures, and lower level policy

Security Policy

- Without policy, current practices are the *de facto* policy
- Like a ship in the night without a lighthouse

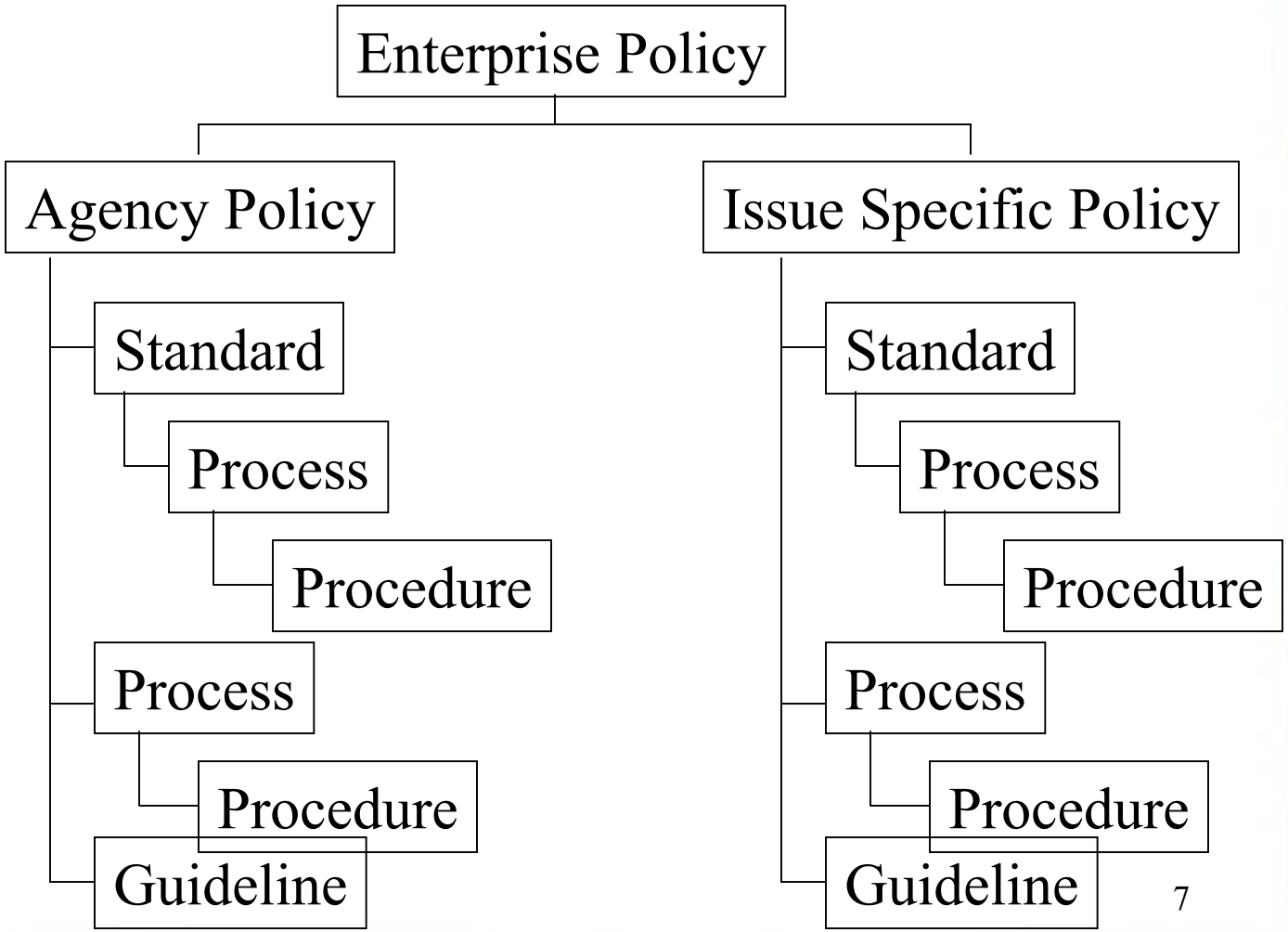
Iowa Policy

- In the past:
  - Multiple agencies, each implementing their own policies
  - No higher level policy guiding a common approach to security
- Today:
  - Multiple agencies, still implementing their own policies
  - Enterprise policy providing consistent guidance to all affected agencies

Policy Hierarchy

- Policy: high level goals and objectives
- Standard: mandatory language supporting policy
- Process: implements a policy or standard
- Procedure: implements a process
- Guidelines: recommendations

Policy Hierarchy



Iowa Enterprise Policy

- 6 sections
  - **Introduction**
  - **Threats**
  - **Security Philosophy**
  - Roles & Responsibilities
  - Policy
  - Glossary

Roles & Responsibilities

- ITD
- Enterprise Information Security Office
- Agency Directors
- Agency CIOs
- Agency Security Officers
- Managers/Supervisors

Roles & Responsibilities

- Users
- Data Custodians
- System Administrators
- Security Administrators
- Database Administrators
- Application Developers

Policy

- Specific policy statements
- Agency practices
- Security, monitoring, business continuity
- Audits and reviews
- Vulnerability and risk assessments
- Life cycle

Policy

- Federal and other higher level requirements
- Incident response
- Physical security
- Security awareness
- Configuration management

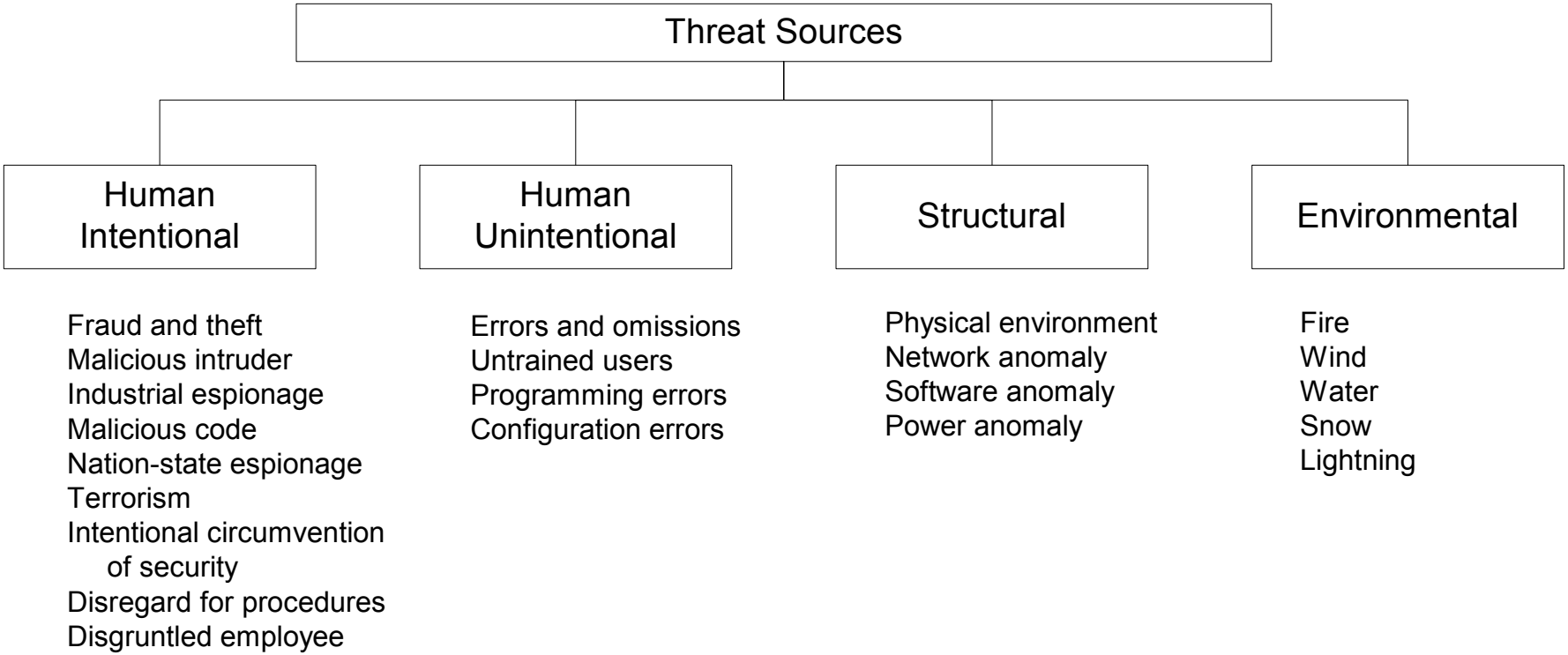
Introduction

- Purpose
- General Policy Statement
- Scope
- Statutory Authority
- Compliance
- Document Changes and Feedback

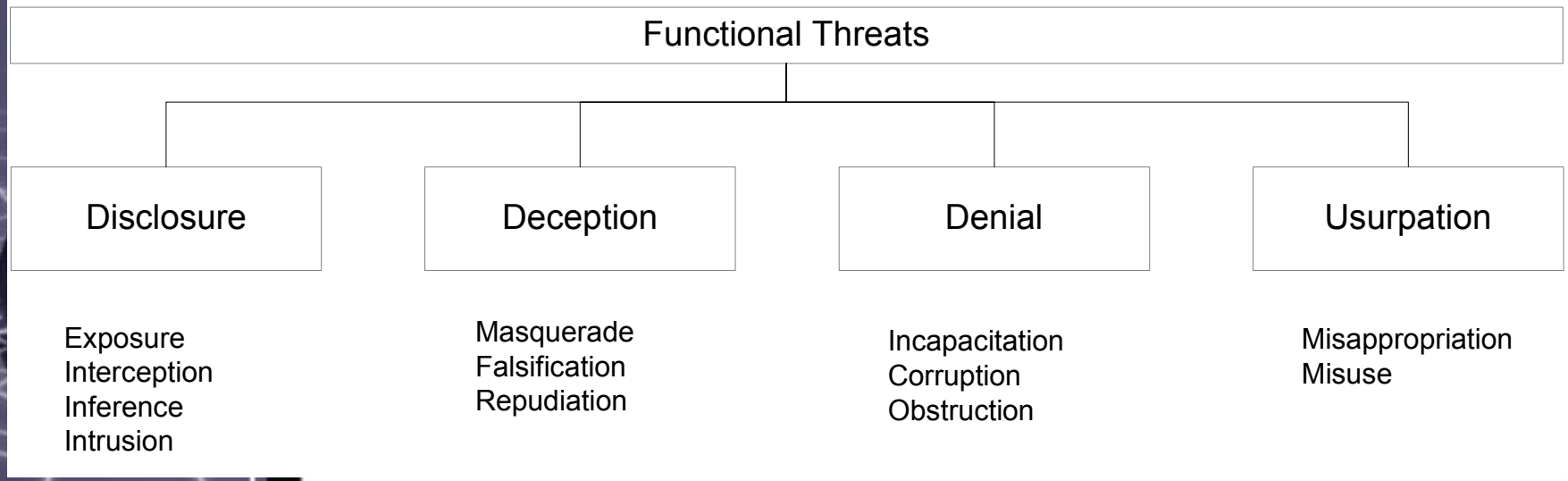
Threats

- Many sources
- Need to consider all threats
- Those things that affect confidentiality, integrity, and/or availability
- Two categories: source & function

Threat Sources



Functional Threats

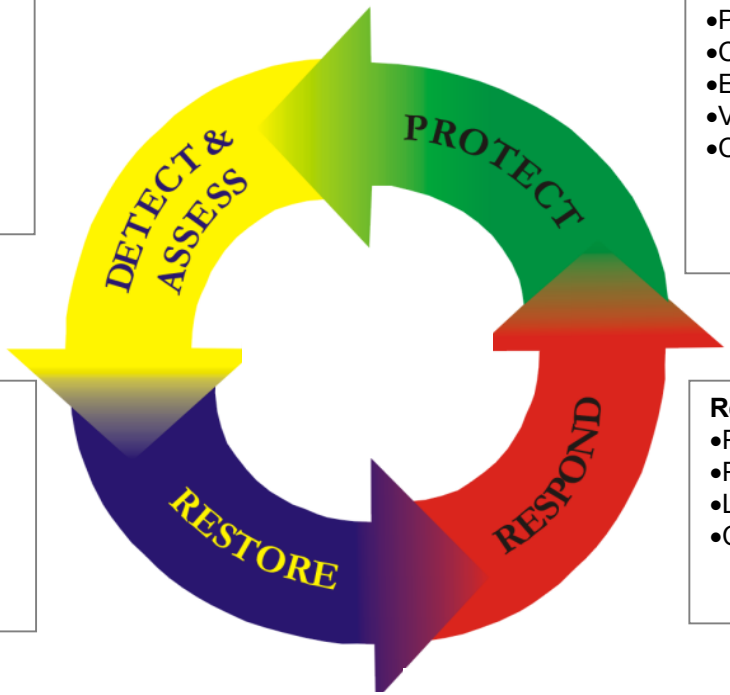


Security Philosophy

- Basic Principles
  - Protect confidentiality, integrity, and availability
  - Security is a critical enabler
- Information Assurance
  - protect and defend information and information systems

Information Assurance

Detect
- Threat identification
- Intrusion detection
- Incident reporting
- Intelligence/law enforcement integration



Protect
- Policies, standards, and procedures
- Certification and accreditation
- Education and training
- Vulnerability assessment
- Countermeasures

Restore
- Incident response
- Business continuity/disaster recovery planning
- Exercise plans

Respond
- Post-attack analysis
- Plan & policy modification
- Law enforcement involvement
- CERT involvement

Security Philosophy

- Defense in Depth
  - Technical and non-technical layers of security
  - Defensive countermeasures reinforce each other
  - No single technique or mechanism is relied upon

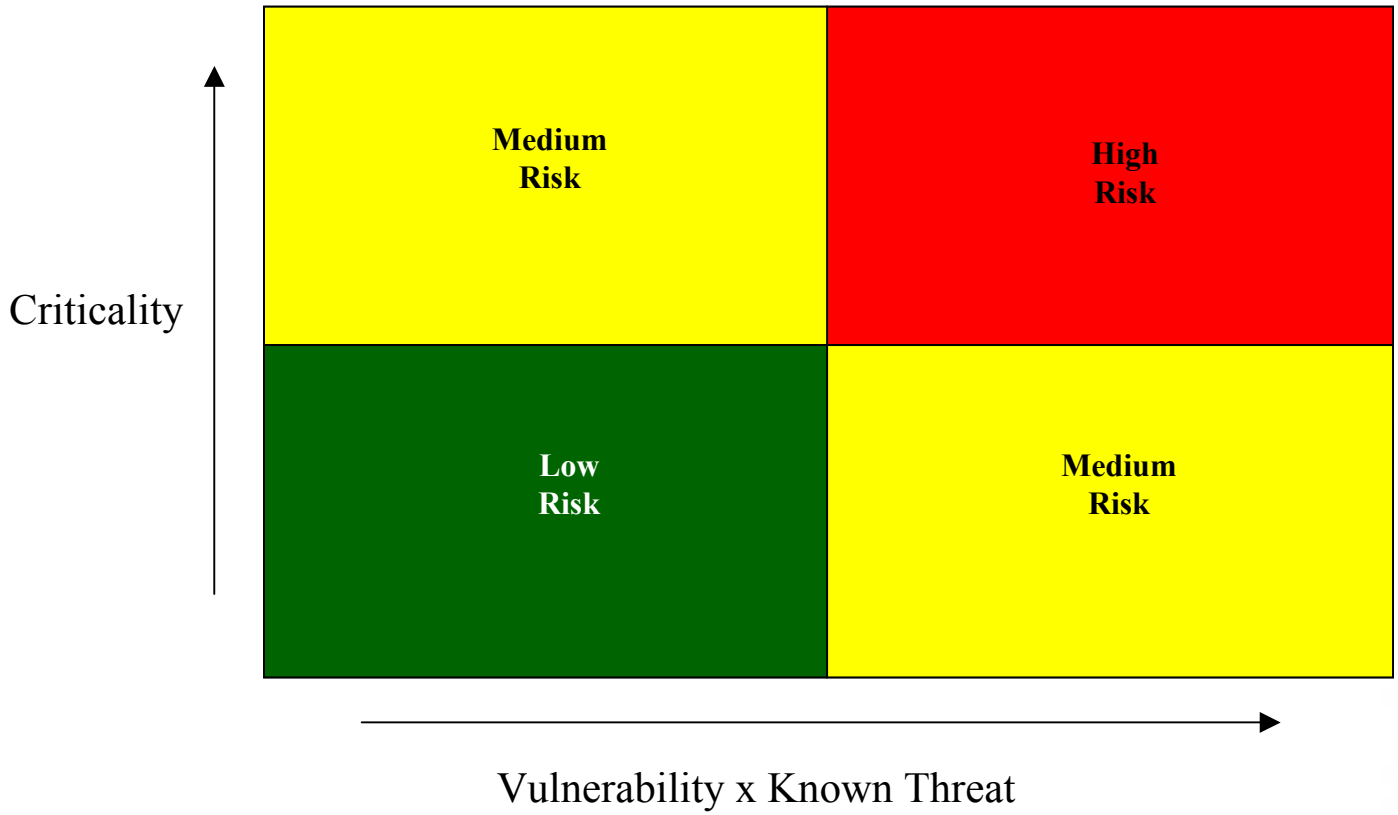
Security Philosophy

- Risk Management
  - Can't eliminate risk
  - So… we mitigate risk (reduce it) to acceptable levels
  - Make risk-based decisions
  - Four questions
    - What can hurt me?
    - How can it hurt me?
    - How critical am I?
    - What can I do to protect myself?

STATE OF IOWA

ITD

Risk



Security Philosophy

- Access Control
  - Access decisions based on identity linked together with a single meta-directory
  - Access control policies orchestrated at a single point and integrated with existing and future technologies
  - Physical & logical
  - Based on roles & responsibilities
  - Decisions at the lowest level required
  - External, internal, server, folder, file, field

Security Philosophy

- Enterprise Information Assurance
  - Enterprise-wide architecture
  - Enforce common philosophies and policies, standards, processes, and procedures
  - Consider security end-to-end

STATE OF IOWA

ITD

Questions?